Capítulo 7
La seguridad de las comunicaciones inalámbricas

1. Presentación

La transmisión de información digital cada vez está más presente en el día a día de las personas. Con esta evolución aparecen las limitaciones, porque los datos transmitidos pueden ser críticos desde el punto de vista de la seguridad o a nivel personal.

Para satisfacer las demandas actuales, las comunicaciones deben ser fiables, seguras, rápidas y prácticas. Dos tecnologías principales compiten para cumplir con estas limitaciones:

– Conexiones alámbricas (cobre, fibra óptica, etc.).

– Enlaces por ondas de radio (Wi-Fi, Bluetooth, etc.).

En el aspecto práctico, la elección se centra obviamente en los enlaces inalámbricos que permiten, como su nombre indica, evitar la conexión de un cable para transmitir información.

La desventaja es que una transmisión de radio se puede escuchar usando cualquier receptor legítimo o pirata. Desde las personas con muy pocos conocimientos hasta especialistas, pueden comprometer las comunicaciones de radio con equipos sencillos listos para usar y que se encuentran sin dificultad en Internet o dispositivos sofisticados y eficientes, reservados para profesionales (si aceptamos llamar 'profesionales' a los piratas de alto nivel).

En la creciente expansión de las comunicaciones inalámbricas, encontramos todos los medios de comunicación tradicionales como el teléfono móvil, wifi, etc. Pero un área en particular se está volviendo cada vez más importante: la IoT (*Internet of Things*: los objetos conectados a Internet).

2. Los objetos conectados

Estos objetos se convierten en un tema muy amplio. La moda actual es conectar todos los accesorios que nos rodean. Pero, ¿qué es un IoT? Un objeto que originalmente tiene una función sencilla y concreta y al que le añadimos la posibilidad de enviar información digital a equipos informáticos.

Los ejemplos son numerosos. Desde la aplicación simple, a veces excéntrica, hasta la aplicación que realmente aporta algo; a los diseñadores no les falta imaginación. No vamos a hacer aquí un inventario de las novedades, sino que nos vamos a centrar en algunos puntos concretos de las tecnologías utilizadas. La primera observación es que las comunicaciones son inalámbricas, por lo tanto, utilizan transmisiones de radio digital. Esta tecnología no es nueva, pero sus evoluciones y su uso intensivo son realmente de nuestro tiempo.

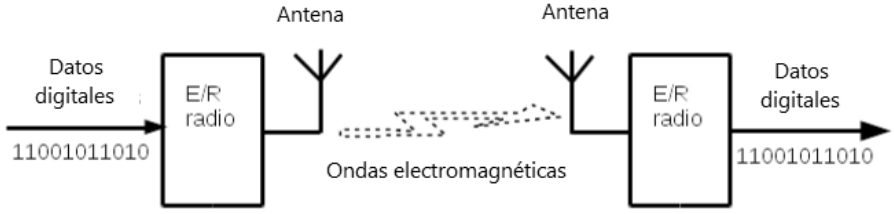
Por lo tanto, algunas nociones son esenciales para comprenderlas y de esta manera dominar mejor las herramientas de prueba, análisis y piratería. Un buen conocimiento permite el desarrollo de estas herramientas, tanto de software como de hardware.

3. Las transmisiones de radio

Evidentemente, aquí el objetivo no es hacer una presentación larga y completa de las técnicas de transmisión de radio, que sin duda sería muy interesante, sino sentar las bases técnicas y el vocabulario utilizado.

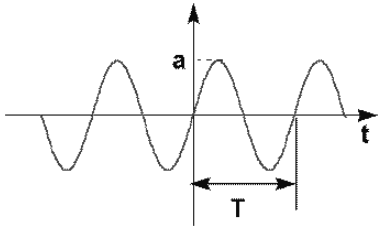
Una transmisión de radio permite enviar y recibir información (digital para nuestro estudio) desde el punto A hasta el punto B sin soporte físico. Las ondas electromagnéticas hacen posible esta comunicación. Por lo tanto, estamos en presencia de dos dispositivos tecnológicos denominados emisor-receptor de radio.

El esquema es muy simple:



Emisor-receptor de radio

La onda electromagnética básica es sinusoidal:



Señal sinusoidal (fuente Internet)

Para lograr transmitir información, es necesario modificar un poco esta onda para diferenciar entre los valores que se envían (en el caso más trivial, el "0" y el "1" lógicos). Al analizar una señal sinusoidal, podemos ver que se caracteriza por su amplitud, su frecuencia y su fase. Desde un punto de vista matemático:

$$S(t) = A \cdot \sin(\omega t + \phi)$$

Ecuación de una señal sinusoidal

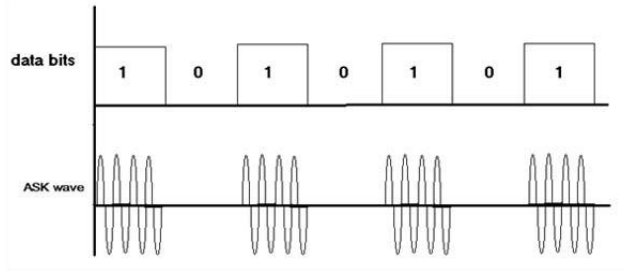
Por lo tanto, es posible modificar su amplitud, su frecuencia, su fase o incluso combinar dos parámetros en función de los datos digitales que se van a transmitir. Decimos que estamos modulando la señal. De hecho, es la famosa función de "modulación" de la que oímos hablar en todas las comunicaciones por radio.

En nuestro ejemplo trivial anterior, podemos imaginar una modulación muy sencilla:

– Se transmite un 0 lógico => A = 0, amplitud nula.

– Se transmite un 1 lógico => A = 1, máxima amplitud.

De esta manera obtenemos una modulación llamada ASK (*Amplitude Shift Keying*, modulación por saltos de amplitud) y más exactamente, en nuestro caso, OO-ASK (*On OffASK*), porque modulamos todo o nada.



Modulación OO-ASK (fuente: www.engineersgarage.com)

Esta tecnología es muy fácil de implementar, pero tiene algunos inconvenientes como la fiabilidad, la velocidad y el alcance.

La escucha y la piratería son muy sencillas y rápidas, ya que no hay dificultades estructurales en el hardware utilizado.

La tasa binaria es baja porque solo se transmite un bit a la vez.

La distancia entre el transmisor y el receptor es modesta, ya que la potencia de transmisión es limitada y aquí no se utiliza ninguna técnica de espectro ampliado.

La modulación ASK todavía se usa en muchas comunicaciones donde la seguridad a nivel de enlace físico no es realmente una prioridad.

Para mejorar las tres restricciones mencionadas anteriormente, es posible utilizar otras técnicas de modulación que proporcionen características muy superiores a las comunicaciones. Estos son algunos de los ejemplos más comunes entre docenas de tecnologías que tienen mejor rendimiento y son más fiables unas que otras.

– FSK: *Frequency Shift Keying*
– PSK: *Phase Shift Keying*
– QPSK: *Quadrature Phase Shift Keying*
– GFSK: *Gaussian Frequency Shift Keying*
– QAM: *Quadrature Amplitude Modulation*

Y para el espectro ampliado:

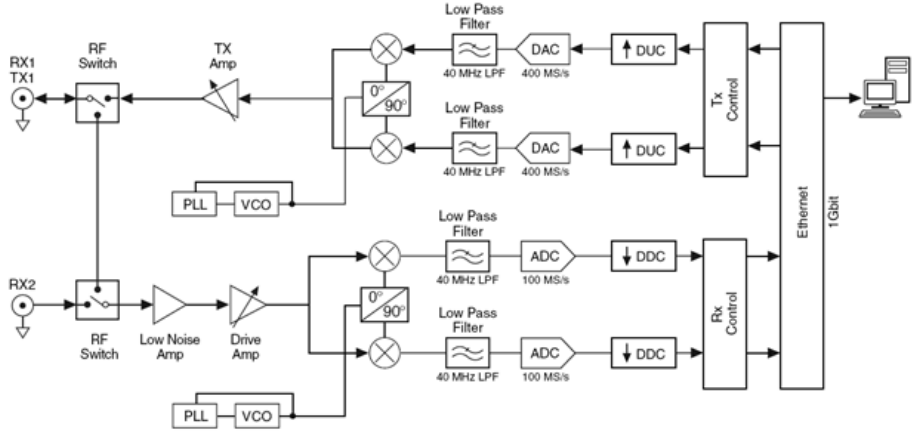
– OFDM: *Orthogonal Frequency-Division Multiplexing*
– DSSS: *Direct Sequence Spread Spectrum*

Como se ha mencionado anteriormente, el propósito de este capítulo no es dar un curso sobre comunicaciones por radio, por lo que respecta a esta sección lo dejaremos aquí. Pero, ¿por qué interesarse por estas nociones científicas y tecnológicas? Sencillamente porque, aunque ya existen muchos equipos y herramientas informáticas, normalmente es obligatorio ensuaciarse las manos y es imprescindible modificar o crear herramientas para adaptarlas a situaciones inéditas.

Existe una tecnología muy interesante para esto, la conversión directa en emisores-receptores digitales.

4. La radio de software

Con el progreso tecnológico, los circuitos electrónicos ahora pueden convertir frecuencias de radio en banda base en rangos de frecuencia relativamente amplios. Y lo que es aún más importante, los convertidores de analógico a digital de gran velocidad permiten un escaneado de alta frecuencia que puede cubrir canales grandes, o incluso varios al mismo tiempo. Con estos circuitos eficientes y económicos, la parte relativa al hardware se convierte en algo muy sencillo y prácticamente genérico, independientemente de cuál sea la comunicación por radio de que se trate. El diagrama principal de un receptor como este, se muestra a continuación:



Emisor-receptor digital NI USRP 2920

Se puede ver que la parte del hardware es relativamente sencilla y que su estructura es bastante genérica. En realidad, esta tecnología crea (recibe) o gestiona (emite) un flujo importante de datos digitales. Esto es lo más interesante, pero también lo más complejo desde el punto de vista del procesamiento digital.

Los datos digitales son la representación de los escaneados resultantes de la conversión analógico/digital que representan el valor real e imaginario de un número complejo, imagen de un valor instantáneo de la señal de banda base. Sin entrar en detalles matemáticos, esta representación permite modular o demodular todas las comunicaciones posibles. Al disponer de un dispositivo de este tipo, solo tiene que establecer el procesamiento digital adecuado para crear "radios basadas en software". Por supuesto, existen programas informáticos listos para usar que permiten la recepción y emisión sin ningún esfuerzo, como, por ejemplo, clonar y reproducir un canal o incluso escuchar estaciones de FM, etc.

La gran ventaja es poder intervenir nosotros mismos para adaptar el procesamiento digital a nuestras necesidades. El diseño o modificación puede ser bastante difícil, pero más o menos factible dependiendo de su nivel de conocimiento sobre la materia, como veremos un poco más adelante en este capítulo.

5. El hardware disponible

La realización de la parte electrónica puede ser una operación posible, pero se trata de un tema irrelevante. Hay suficiente hardware disponible, con diversas prestaciones y precios, para poder evitar la fase de fabricación. A continuación, se presenta una lista no exhaustiva del más utilizado.

5.1 La llave RTL-SDR

SDR: *Software-Defined Radio* (radio definida por software)

Este receptor DVB-T es un "dongle" esencial para principiantes. Su precio es muy asequible, de 10 a 30 euros, y sus características permiten ciertas manipulaciones. Su gran defecto es que no permite la emisión.

Llave RTL-SDR

Sus principales características son las siguientes:

– Banda de frecuencia: 30 - 1700 MHz.

– Muestreo: 2 MHz.

Gracias a estos parámetros, este circuito permite escuchar y decodificar muchas comunicaciones como radios AM/FM, controles remotos de 433Mhs 868 MHz y muchos otros.

Sin embargo, su límite de frecuencia (alrededor de 1,7-2,0 GHz) no permite llegar a la banda ISM (industrial, científica y médica) de 2,4 GHz donde se producen muchas comunicaciones como el Wi-Fi, el Bluetooth, NRF24, el ZigBee, etc.

5.2 El HackRF One

El principal interés de HackRF es que permite emitir. Tiene unas prestaciones superiores a la llave TNT, lo que hace posible escuchar o emitir comunicaciones prácticamente en todas las bandas ISM clásicas. Su precio oscila entre los 300 y 400 euros.

El HackRF One

Sus características son las siguientes:

- Half-duplex transceiver (Emisor Half-duplex).
- Operating frequency: 10 MHz a 6 GHz (rango de frecuencia de trabajo).
- Supported simples rates: 2 Msps a 20 Msps (cuadratura) (frecuencias de muestreo).
- Resolution: 8 bits.
- Interface: High Speed USB (with USB Micro-B connector).
- Power supply: USB bus power.

La primera característica indica que el HackRF es un emisor half-duplex (emisión o recepción, pero no ambas a la vez), lo que supone una desventaja para determinadas aplicaciones como la integración en una red o la puesta en marcha de un Man In The Middle.

Potencia de transmisión:

- 10 MHz to 2150 MHz 5 dBm to 15 dBm, generally increasing as frequency decreases.
- 2150 MHz to 2750 MHz: 13 dBm to 15 dBm.
- 2750 MHz to 4000 MHz: 0 dBm to 5 dBm, increasing as frequency decreases.
- 4000 MHz to 6000 MHz: -10 dBm to 0 dBm, generally increasing as frequency decreases.

Como puede comprobar, la potencia de la parte emisora no permite actuar en comunicaciones extendidas. Es suficiente para realizar pruebas y depuraciones en local que se pueden utilizar con otras soluciones más potentes.